



International Association of Jewish Genealogical Societies (IAJGS)

6052 Hackers Lane Agoura Hills, CA 91301

818-889-6616 tel 818-889-0189 fax

www.iajgs.org

STATEMENT FOR THE RECORD, U.S. HOUSE OF REPRESENTATIVES COMMITTEE WAYS & MEANS, SUBCOMMITTEES ON OVERSIGHT AND SOCIAL SECURITY, MAY 8, 2012 JOINT HEARING ON IDENTITY THEFT AND TAX FRAUD

I. INTRODUCTION:

The U.S. House of Representatives Ways and Means Subcommittees on Oversight and Social Security held a joint hearing on 8 May 2012, on Identity Theft and Tax Fraud including the accuracy and uses of the Social Security Administration's Death Master File. The genealogical community was not extended an invitation to testify at the hearing, however, public comments were solicited. This statement is accordingly submitted.

II. IAJGS BACKGROUND & CONTACT INFORMATION:

The International Association of Jewish Genealogical Societies is the umbrella organization of 70 genealogical societies and Jewish historical societies worldwide whose approximately 10,000 members are actively researching their Jewish roots. We want to ensure that our members will be allowed continued and maximum access to these records. The IAJGS and its predecessor organization were formed in 1988 to provide a common voice for issues of significance to its members and to advance our genealogical avocation. One of our primary objectives is to promote public access to genealogically relevant records. In 2012, we are holding our 32nd consecutive annual International Conference on Jewish Genealogy (www.iajgs.org).

IAJGS is a voting member of the Records Preservation and Access Committee (RPAC) that is a joint committee whose other voting members include The National Genealogical Society (NGS) and the Federation of Genealogical Societies (FGS). The Association of Professional Genealogists (APG), the Board for Certification of Genealogists (BCG), and the American Society of Genealogists (ASG) also serve as participating members. RPAC also includes participation from several of the commercial providers of genealogical information.

Contact Information:

IAJGS official mailing address is:

IAJGS

PO Box 3624

Cherry Hill, NJ 08034-0556

However, for purposes of this statement please use the following contact information:

Jan Meisels Allen,

Vice President, IAJGS

6052 Hackers Lane Agoura Hills, CA 91301 (818) 889-6616 tel (818) 991-8400 fax (call before submitting a fax)

e-mail: vicepresident@iajgs.org

Officers

Michael Goldstein, Jerusalem, Israel,

Jan Meisels Allen, Agoura Hills, CA, USA,

Joel Spector, Cherry Hill, NJ, USA,

Paul Silverstone, New York, NY, USA,

Immediate Past President

Anne Feder Lee, Honolulu, HI, USA,

President@iajgs.org

Vicepresident@iajgs.org

Secretary@iajgs.org

Treasurer@iajgs.org

Anne@iajgs.org

Directors-at-large

Nolan Altman, Oceanside, NY, USA,

Daniel Horowitz, Kfar Saba, Israel,

Kahlile Mehr, Bountiful, UT, USA,

Mark Nicholls, Edgeware Middlesex, UK

Jay Sage, Newton Center, MA, USA

Jackye Sullins, Carlsbad, CA, USA,

Nolan@iajgs.org

Daniel@iajgs.org

Kahlile@iajgs.org

Mark@iajgs.org

Jay@iajgs.org

Jackye@iajgs.org

Previous Hearings

The Social Security Subcommittee held a hearing on the issue on 2 February 2012, and the Senate Finance Committee Fiscal Responsibility & Economic Growth Subcommittee also held a hearing on 20 March 2012. IAJGS submitted Statements for the Record for the 2 February 2012 and 20 March 2012 hearings. These previous Statements are incorporated by reference into this statement.

Introduction

Thank you for the opportunity to present the IAJGS concerns regarding the Subcommittees' proposed reduction or elimination of public access to the commercial version of the Death Master File (DMF), the Social Security Death Index (SSDI). For the purposes of this statement, we will be addressing access to the SSDI rather than the DMF, as the SSDI is the version that genealogists are permitted to access.

It is ironic that a system that is used to prevent identity theft (by permitting employers, financial organizations, insurance companies, pension funds, and others the ability to check names against those deceased as reported on the Death Master File), [<http://www.ntis.gov/products/ssa-dmf.aspx>], is now being determined—inappropriately—as an instrument of identity theft.

We support the Subcommittees' intent to protect the residents of the United States from improper usage of their personal information, and to protect them from identity theft. We support, the provisions in S1534, H 3215 and HR 3482 which propose strong criminal penalties for those who willfully misuse or disclose another's personal tax identity number (Social Security Number) resulting in a personal gain. Only strong criminal penalties will hopefully, deter those who are misusing another's Social Security Number (SSN) for their own gain.

Violations occur due to computer breaches from government and private enterprises and government and private enterprise personnel misusing or stealing Social Security numbers. A recent study (2012) by ID Analytics estimates of 100 million applications examined to the entire annual volume of applications submitted for credit products and services in the U.S., that nearly 6.8 million applications have at least a partial match to the DMF. Many of these—roughly 2.4 million—are simply SSN typos. Approximately 1.6 million applications are instances of a fraudster using a fabricated SSN that **unintentionally** matches the SSN of a deceased person¹. A 2009 study stated “in the last five years, approximately 500 million records containing personal identifying information of United States residents stored in government and corporate databases was [sic] either lost or stolen”¹. Many computer breaches have been well documented in the press.² In addition, there have been newspaper accounts of Social Security numbers found in dumpsters and other places³ where they can be easily found and used by “fraudsters”.

Genealogists Are Not the Cause of Identity Theft

Genealogists rely on the Death Master File/Social Security Death Index for legitimate reasons. Their access to the SSDI is not the cause of identity theft. Thieves are the cause of identity theft. Preventing genealogists access to the SSDI will not prevent the aforementioned type of illegal use of SSNs. Financial institutions and government agencies have been hacked into numerous times and that has been documented^{1,2}, but was not mentioned during the hearing. Nor was there mention of returning to using non-computerized data to avoid the inevitable hacking that occurs daily in the 21st century. If we accept the continued use of computerized data, and the continued likelihood of hacking occurring to any given database at any time, then we must also accept that, occasionally, misuse of data will occur. This is why it is imperative that the IRS take more aggressive action to prevent fraudsters from using fraudulently obtained SSNs on fraudulently filed tax returns. It is not reasonable, constitutional, or in the nation's interests, to remove public documents from public access. For a real solution to this problem, see below “IRS Needs to be More Proactive.”

In Mr. J. Russell George, Treasury Inspector General for Tax Administration statement before the joint subcommittees' hearing, he commented: “ The IRS began a pilot program in Processing Year 2011 which locked taxpayers' accounts where the IRS Master File and Social Security Administration data showed a date of death. The IRS places a unique identity theft indicator on deceased individuals' tax accounts to lock their tax account.” While it is gratifying that, the IRS is **finally** using Social Security Administration information to prevent tax identity fraud—it is unfortunate that the IRS was not using the DMF information all along to prevent fraudulent filings of deceased individuals.

What was even more striking in Mr. George's statement was that the tax identity fraud of living individuals was the overwhelming cause of identity theft and tax fraud, including the billions of dollars of falsely used debit cards and not depositing refunds directly into the taxpayers' bank accounts. These fraudulent practices by the living are not part of the DMF—and therefore, the focus of closing the commercial version, the Social Security Death Index, appears as if it will have no impact at all on the overwhelming problem of identity theft and tax fraud. Therefore, we ask, why are the Subcommittees focused on the SSDI when closing that off will have virtually no bearing on the overwhelming problem.

Detective Sol Augeri noted, in his oral statement during the March 20th hearing before the Senate Finance Committee Subcommittee on Fiscal Responsibility and Economic Growth, that once the genealogical websites withdrew the SSDI from public access, identity theft did not abate. Rather, Detective Augeri said the access to Social Security Numbers to be used in identity theft moved to institutions: hospitals, nursing homes, physician offices and other institutions. In his written statement, Detective Augeri said "...they turned to individuals who [sic] worked in Assisted Living Facilities who would obtain necessary information on patients. Lists of names are now being sold by those having access to personal information in businesses, medical offices, and schools." This documents that removal of the SSDI from public access does not necessarily reduce the problem of fraudulent use of a Social Security number. Indeed, we heard at the March 20th hearing that identity theft continues to grow, in spite of genealogy and family history sites' removal of the SSDI from public access. For example, medical identity theft, whereby medical employees have been found to steal patient's identification has become a growing business.⁴ If Congress limits public access to SSDI, it will no longer be available as a reference check to many who use it as an identity theft deterrent, there well may be an increase in identity theft.

Loss of Critical Data in Death Master File If States Prevent Inclusion in the Commercial Version

Many organizations—state and local government, financial, insurance and other businesses—rely on the SSDI for fraud prevention. Recently, the New York City Employee Retirement System started a new system comparing the SSDI with their pension data bank. This was initiated due to a number of recent fraudulent pension filings⁵. As states assert their rights to retain control over the sale of their data in the SSDI, the recent notification from over 30 states that state data can no longer be included in the SSDI is of compelling concern. The elimination of data from the SSDI raises the concern about the resulting loss of a meaningful fraud deterrent used by various organizations including state and local government as well as financial, insurance, medical and other businesses. How do the Subcommittees plan to "replace" this effective fraud deterrent?

Interest in Family History/Genealogy

Millions of Americans are interested in their family history. The Harris Interactive Poll taken in August 2011 found that four in five Americans have an interest in learning about their family history. The Poll also reported 73% of Americans believe it is important to pass along their family's lineage to the next generation.⁶ Genealogists doing U.S. research located both in and outside the United States rely on the Social Security Death Index.

Certification for Certain Genealogists With Need For Immediate Access to the Death Master File/Social Security Death Index

While IAJGS advocates all genealogists should have immediate access to the SSDI, we would support the two year delay in access as proposed in S 1534, HR 3215 and HR 3482-and if necessary the third year that National Taxpayer Advocate Nina Olson advocated during her oral testimony during the May 8th and March 20th hearings. This support is based on amending the bill to include that certain genealogists are to be eligible for certification for immediate access under the bills' provisions. These genealogists include:

- Forensic genealogists. These are genealogists who work, for example by contract on specific cases with the Department of Defense in identifying next of kin of deceased military personnel from prior conflicts and working with local, county, and state coroners to help find the next of kin of deceased in order for the deceased to have a proper burial;
- Heir researchers who are working under contract with law firms to prove or disprove that someone is eligible as part of a deceased's estate or Native American tribal funds;

- Those researching **individual** genetically inherited diseases to help current and future generations obtain necessary medical testing to determine if they currently need prophylactic treatments. We are aware that medical researchers may already be eligible for certification, but many work with aggregate data and the individual needs to know about their own medical genetically inherited history.

While some organizations currently are certified for immediate access, individual genealogists working within the above three categories are not covered and certification for immediate access needs to be specifically addressed in the legislation. The Records Access and Preservation Committee, which is described on page one of this statement, is willing to work with the Subcommittees in determining who would qualify.

See below for more detail.

Family Medical History

Genealogists use Social Security Numbers (SSNs) to appropriately identify records of people when tracing **family medical history**, especially if the person has a common name: Sara Cohen, Tom Jones, Jose Martinez, Mary Smith, etc. During the March 20th hearing before the Senate Finance Subcommittee on Fiscal Responsibility, it was mentioned that perhaps genealogists could make do with the last four digits of the Social Security Number. Unfortunately, this was proven not to be true in the February 2nd House Subcommittee on Social Security hearing. Mr. Pratt, representing the Consumer Data Industry Association (CDIA), mentioned CDIA had conducted a study and found some people with common names, i.e. Smith, also had the same last four digits on their Social Security number, validating why the complete Social Security number is necessary.

Genealogy assists researchers in tracing family medical problems that are passed on from generation to generation. Information included in birth, marriage, and death records is critical to reconstructing families and tracing genetically inherited attributes in current family members. The SSN is essential to make certain that one is researching the correct person. Increasing numbers of physicians are requesting that their patients provide a “medical family tree” in order to more quickly identify conditions common within the family ⁷. Information on three generations is the suggested minimum. The US Surgeon General includes preparing a family medical history as part of the American Family Health Initiative ⁸.

There are many genetically inherited diseases, but for the purposes of this statement, we will mention the *BRCA1* and *BRCA2* genes’ mutations and breast and ovarian cancer. The following information is from the National Cancer Institute ⁹.

“A woman's risk of developing breast and/or ovarian cancer is greatly increased if she inherits a deleterious (harmful) *BRCA1* or *BRCA2* mutation. Men with these mutations also have an increased risk of breast cancer. Both men and women who have harmful *BRCA1* or *BRCA2* mutations may be at increased risk of other cancers.

The likelihood that a breast and/or ovarian cancer is associated with a harmful mutation in *BRCA1* or *BRCA2* is highest in families with a history of multiple cases of breast cancer, cases of both breast and ovarian cancer, one or more family members with two primary cancers (original tumors that develop at different sites in the body), or an Ashkenazi (Central and Eastern European) Jewish background.

Regardless, women who have a relative with a harmful *BRCA1* or *BRCA2* mutation and women who appear to be at increased risk of breast and/or ovarian cancer because of their **family history** [emphasis added] should consider genetic counseling to learn more about their potential risks and about *BRCA1* and *BRCA2* genetic tests.

The likelihood of a harmful mutation in *BRCA1* or *BRCA2* is increased with certain familial patterns of cancer [emphasis added]. These patterns include the following for women of Ashkenazi Jewish descent:

- Any first-degree relative diagnosed with breast or ovarian cancer; and
- Two second-degree relatives on the same side of the family diagnosed with breast or ovarian cancer.”

This form of breast cancer is something not unique to Ashkenazi Jews. Studies have demonstrated that this has also been found in the Hispanic communities of New Mexico and Colorado--who did not know they

were descended from Sephardic Jews who had hidden their Jewish identity to survive the Inquisition in the 15th century. This is described in Jon Entine's *Abraham's Children: Race, Identity and the DNA of the Chosen People*, by the Smithsonian in their article, *The Secret Jews of San Luis Valley*, and *The Wandering Gene and the Indian Princess: Race, Religion, and DNA*¹⁰

People who have had members of their families diagnosed with breast cancer need to know whether past family members may have also died from this disease, in order to determine if it is inherited. Both current and future generations need to have this information in order to make decisions about whether to prophylactically remove both breasts and ovaries (which can mean the difference between early detection and treatment versus possible early death). This is something both men and women need to be able to research--as either can be carrying the gene mutation. The SSDI is a critical tool in assuring researchers that the records they have located on possible ancestors are indeed the correct persons, especially when they have a common name.

We use this as only one example of inherited diseases that require the ability to research ancestry using a SSN—regardless of ethnicity.

Working with Coroners to Identify Deceased's Next of Kin

People are going to their graves with no family to claim them. Medical examiners and coroners' offices—frequently overstretched with burgeoning caseloads—need help in finding next of kin of the deceased. The deceaseds' identities are known; it is their next of kin that are unknown in these cases. Over 400 genealogists are now offering their volunteer services to help locate the next of kin for unclaimed persons. The identities of these people are known, but the government agencies are not always able to find the families, so they are literally unclaimed. It is a national problem with which coroners must cope. See unclaimedpersons.org

Working with the Military

There are literally tens of thousands of United States Veterans' remains left unclaimed throughout the Nation. Sometimes decades pass while these remains are waiting to be identified as Veterans and given a proper military burial. Genealogists work with the military to locate relatives of soldiers who are still unaccounted for from past conflicts. By finding relatives, the military can identify soldiers using DNA, and notify the next of kin so the family can make burial decisions. While using DNA, the genealogists also need SSNs to help assure they are finding the correct person's family¹¹.

Genealogy as a Profession

While there are millions of people who actively study and research their family history as an avocation, there are many others who earn their livelihoods as professional genealogists. Professional genealogists use the SSDI to (1) help track heirs to estates, (2) find title to real property, (3) find witnesses to wills that need to be proved, (4) work on the repatriation projects [see Working with the Military], (5) track-works of art—including stolen art—and repatriation of looted art work during the Nazi era of World War II, and (6) assist in determining the status of Native American tribes and tribal members to prove—or disprove—that they are entitled to share in Tribal casino revenues.

IRS Needs to Be More Proactive

While we are heartened that the IRS has begun a fraud identification program in 2011 with various new identity theft screening filters -- this is not enough. They need to do more to work with the identity theft victims and even more to prevent identity theft—which includes more flagging of returns of not only the deceased, but of others covered under the same tax return: spouses and dependents. This “simple” notation in the file can further prevent tax refunds being generated by the fraudulent filer. It is a positive outcome that the IRS has undertaken various preventive activities. However, much more is required to address the growing blight of identity theft and actions need to be undertaken now.

If the IRS were to routinely run Social Security numbers included in tax returns against the Death Master File, they might avoid giving refunds to deceased individuals. This is a data match between two government computer programs—something that should be routinely undertaken. The difference between data security and data stewardship is excellently described in Kenneth Ryesky's statement to the Subcommittee relative to the

March 20th and May 8th hearings. Ryesky testified that, along with failure of the IRS for data stewardship, “The social security numbers (SSNs) were not verified, even though the means to verify the numbers should have been readily available to the IRS... data security practices alone do not constitute sound stewardship of taxpayer personal data.”¹²

“Operation Rainmaker” (also known as Operation TurboTax), was a tax fraud operation in the Tampa Bay area as discussed by Tampa Police Department Lieutenant Augeri during the Senate Finance Subcommittee hearing. Law enforcement interviews specified that the IRS, while cooperating with other law enforcement officers, is not authorized to share information with local law enforcement departments, hampering efforts to protect their citizens. If the federal government is serious about addressing identity theft that uses a person’s Social Security number, then the IRS needs to be given legislative authority to share information with local, county, and state law enforcement organizations. Perhaps as a minimum, the subcommittees through legislation can adopt the suggestion by National Taxpayer Advocate Olson in her written and oral statements for both the May 8th and March 20th hearings, that the identity theft victim be able to receive the “bad return”. Currently, this is a pilot project where information filed by the alleged identity thief, enabling the victim to then provide the information to local law enforcement or provide a release for the IRS to share the information directly with local law enforcement. It was also stated that filing tax refunds for under \$10,000 will not get any attention. As “Operation Rainmaker” found the average tax, fraud was about \$9,500, below the \$10,000 threshold¹³. This is another practice that the Congress needs to review, as the criminals who are perpetrating this fraud know they will be undetected!

It became apparent through Mr. McClung in his testimony at the Senate Finance Subcommittee's 25 May 2011 Hearing,¹⁴ together with the testimony of Mr. Agin at the House Ways & Means Subcommittee's 2 February 2012 Hearing,¹⁵ that the IRS assumes the first person filing is the “legitimate” filer and by inference, the second filer is the fraudulent party. The IRS needs to amend their practice to require some verification to determine which is a valid filing, when the filing involves a deceased child.

Unfortunately, since the IRS advocated electronic filing of tax returns, one unexpected consequence is the remarkable increase in tax identity theft.

Support For Efforts to Cease Identity Theft

- If income tax returns were electronically compared to the Master Death File, matching cases could be flagged for special processing, and the person attempting to create a tax fraud could be stopped before the fraud occurs.
- A parent’s social security number should be required when filing a tax return for any minor. It is an extremely rare occurrence that a minor child would not be listed as a dependent on the parent or guardian’s tax filing. If the minor dies, the IRS could have a procedure to flag any filings without the parent’s social security number, again preventing the fraud. Draft legislative language developed by the Records Preservation and Access Committee¹⁶ (see Attachment A) would facilitate just this prevention of identity theft perpetrated on children. The *National Taxpayer Advocate’s Report to Congress for 2011* specifically highlights the benefits of the IRS Issued Identity Protection PINs¹⁷ and suggests that taxpayers should be allowed to turn off their ability to file tax returns electronically. Any family that suffers a death could elect to turn off the electronic filing ability.
- Criminal penalty statutes for those who fraudulently use Social Security Numbers, including, but not restricted to, those who misuse their positions (e.g., hospital, medical institution and office personnel, financial and credit card organizations personnel, prison corrections officer, college or university registrar etc.)

For the reasons stated above:

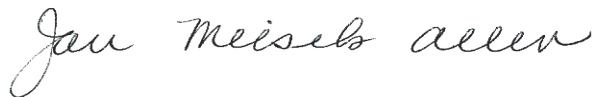
- Genealogists are **NOT** the cause of identity theft;
- Genealogists have legitimate, professional and life saving reasons to have immediate access to the SSDI; and

- Proactive measures are needed to prevent identity theft and vigorously pursue and punish the **TRUE** identity thieves, and
- “Fraudsters” are focusing on stealing the Social Security Numbers of live people not the dead-- when fraudulent tax filings are being rendered to the IRS; and
- SSDI is a deterrent to fraud and removing access to this database will cause more harm than good.

IAJGS respectfully and vehemently encourages the Subcommittees to continue public access to the commercial version of the Death Master File, known as the Social Security Death Index, to be available to the public. If any time period for withholding this from the public is required, then it should not be greater than two or three years including the year of death with certain genealogists being eligible for certification for immediate access to the Death Master File.

On behalf of the International Association of Jewish Genealogical Societies, we appreciate the opportunity to submit our comments, and for the occasion to bring to the Subcommittees’ attention the many services the genealogy community performs for local, state, and federal government offices. We look forward to working with the Subcommittees and staff to find an accommodation that provides genealogists with immediate and reasonable access to the SSDI.

Respectfully submitted,



Jan Meisels Allen
IAJGS Vice President
Chairperson, IAJGS Public Records Access Monitoring Committee

Endnotes

- ¹ <http://www.idanalytics.com/news-and-events/news-releases/2012/4-23-2012.php>
<http://www.identitytheft.info/breaches09.aspx>
- ² http://www.boston.com/business/articles/2008/03/18/grocer_hannaford_hit_by_computer_breach/
http://www.ncimes.com/news/local/article_3b98ce38-f048-597e-9a76-47321d114326.html
http://www.qctimes.com/news/local/article_06d38e24-146a-11df-91c6-001cc4c03286.html
http://www.washingtonpost.com/politics/tricare-military-beneficiaries-being-informed-of-stolen-personal-data/2011/11/23/gIQAcRNHtN_story.html
<http://sundayherald.com/news/heraldnews/display.var.2432225.0.0.php>
Understanding Identity Theft: Offenders’ accounts of their lives and crimes. Criminal Justice Review, Copes, H., and Vieraitis, L.M. (2009) 34(3), 329-349.
- ³ <http://www.ksat.com/news/Personal-documents-found-in-trash-can/-/478452/8282132/-/59y7ox/-/index.html>

- <http://www.phiprivacy.net/?p=5405>
http://www.abc15.com/dpp/news/region_northern_az/payson/state-agency-leaves-arizonans-sensitive-documents-in-dumpster
<http://www.databreaches.net/?p=16205>
<http://www.vcstar.com/news/2012/mar/30/lost-data-may-have-exposed-800000-people-in/>
4 <http://consumerist.com/2010/03/id-theft-ring-used-hospital-records-for-300k-shopping-spree.html>;
http://articles.sun-sentinel.com/2010-11-11/health/fl-hk-holy-cross-id-20101110_1_identity-theft-ring-patient-files-emergency-room
<http://www.miamiherald.com/2011/12/07/2536190/miami-va-hospital-employee-charged.html>;
5 <http://www.dnainfo.com/new-york/20120509/new-york-city/family-of-dead-city-workers-stole-nearly-400k-pension-cash-report-says>
6 <http://corporate.ancestry.com/press/press-releases/2012/01/ancestry.com-partners-with-historical-society-of-pennsylvania-to-bring-the-states-rich-history-online/>
This survey was conducted online within the United States by Harris Interactive via its QuickQuery omnibus product on behalf of Ancestry.com from August 5-9, 2011 among 2,950 adults ages 18 and older
7 Mayo Clinic staff: "Medical History: Compiling your medical family tree,"
<http://www.mayoclinic.com/health/medical-history/HQ01707>;
8 <https://familyhistory.hhs.gov/fhh-web/home.action>
9 <http://www.cancer.gov/cancertopics/factsheet/Risk/BRCA>
10 *Abraham's Children: Race, Identity, and the DNA of the Chosen People.* Jon Entine, Grand Central Publishing, New York, N.Y. 2007.
<http://www.smithsonianmag.com/science-nature/san-luis-valley.html>
The Wandering Gene and the Indian Princess: Race, Religion, and DNA. Jeff Wheelwright. WW Norton & Co. New York, NY, 2012.
11 <http://www.aarp.org/relationships/genealogy/info-06-2011/genealogy-tips.html>
<http://www.familiesforforgottenheroes.org/Genealogist.htm>
12 Kenneth H. Ryesky, Esq., Statement for the Record, United States Senate Committee on Finance, Subcommittee on Fiscal Responsibility & Economic Growth, Tax Fraud by Identity Theft, Part 2: Status, Progress, and Potential Solutions March 20, 2012.
Kenneth H. Ryesky, Esq. Statement for the Record, United States House of Representatives, Committee on Ways and Means, Subcommittees on Oversight and Social Security, Joint Hearing on Identity Theft and Tax Fraud May 8, 2012
13 <http://www.youtube.com/watch?v=gpgTFO7nMBk>
14 Statement of Terry D. McClung, Jr., Hearing on the Spread of Tax Fraud by Identity Theft: A Threat to Taxpayers, A Drain on the Public Treasury, United States Senate Committee on Finance, Subcommittee on Fiscal Responsibility and Economic Growth (25 May 2011).
<http://finance.senate.gov/imo/media/doc/Testimony%20of%20Terry%20McClung.pdf>
15 Statement of Jonathan Eric Agin, Esq., Hearing on the Accuracy and Uses of the Social Security Administration's Death Master File, House Committee on Ways and Means Subcommittee on Social Security (2 February 2012), http://waysandmeans.house.gov/UploadedFiles/Agin_Testimony202ss.pdf.
16 The Records Preservation and Access Committee is a joint committee, which today includes The National Genealogical Society (NGS), the Federation of Genealogical Societies (FGS) and the International Association of Jewish Genealogical Societies (IAJGS) as voting members. The Association of Professional Genealogists (APG), the Board for Certification of Genealogists (BCG), the American Society of Genealogists (ASG), ProQuest and Ancestry.com also serve as participating members.
17 <http://www.irs.gov/pub/irs-pdf/p2104.pdf>

Attachment A

To address the tax issues surrounding the misuse of Social Security Numbers, the following language captures the concept that if a child under the age of 18 has their social security number associated with that of their parents or legal guardian, and if that information is afforded to the Internal Revenue Service, then administrative procedures may be put in place that would flag claims where the social security number of the deceased child did not match the social security numbers of its parents and appropriate action may be taken by the IRS, as follows:

Existing law requires the Social Security Administration to release the data contained in the Death Master File and arrange it for publication according to *Perholtz v. Ross*, C.A. Nos. 78-2385, 78-2386 D.D.C. Since that time, the data contained in the Death Master File has been widely used to prevent identity theft for fraudulent purposes through the wide dissemination of the information that the person identified with a uniquely identifying Social Security number is deceased.

This bill would require the Social Security Administration to add additional information to the Death Master File to be shared with the Internal Revenue Service for the purpose of prohibiting the criminal act of claiming unrelated deceased dependents.

- 1 SECTION 1. (1) The Commissioner of the Social Security Administration shall arrange and
2 permanently preserve the social security numbers of dependent children with the associated
3 social security numbers of their legal parents or guardians for all applications registered.
- 4 (2) The Commissioner of Social Security may release the indices and data files described in
5 paragraph (1) to the Internal Revenue Service. The Internal Revenue Service having obtained
6 the index pursuant to this paragraph may not release any portion of its contents to any other
7 party or government agencies.
- 8 (3) The Internal Revenue Service or other government agency may not sell or release Social
9 Security indices prepared and maintained by the Social Security Administration except as
10 authorized by law.
- 11 (4) In addition to the indices prepared pursuant to paragraph (1), the Commissioner of
12 Social Security shall prepare separate non-comprehensive electronic indices of all deceased
13 individuals with Social Security numbers that shall be made available for public inspection.
- 14 (5) For purposes of this bill, the following definitions apply:
 - 15 (a) "Data files" means computerized data compiled from Social Security Applications
16 registered with the Social Security Administration.
 - 17 (b) "Person" means any individual, firm, corporation, partnership, limited liability
18 company, joint venture, or association.
 - 19 (c) "Personal identifying information" means first name, middle name, last name,
20 mother's maiden name, and father's surname, and a social security number that is
21 contained in the file.
 - 22 (d) "Financial institution" means any commercial bank, trust company, savings and
23 loan company, insurance company, or person engaged in the business of lending money.
 - 24 (e) "Commercial or non-profit company" means any company or not-for-profit organiza-
25 tion engaged in sharing information about deceased individuals for the pursuit of heir
26 searches, genetic research, blood quantum research, genealogy or family history research,
27 or other legal uses of the information as authorized by law.
- 28 (6) The Social Security Death Master File as presently constituted will be made available
29 for a reasonable fee to financial institutions, commercial companies, non-profit organizations
30 and educational institutions as authorized by law.
- 31 (7) Any person who, in violation of this section, uses, sells, shares, or discloses any informa-
32 tion provided pursuant to this section, or who uses information provided pursuant to this
33 section in a manner other than as authorized pursuant to this section, may be subject to the
34 assessment of a civil penalty by the Internal Revenue Service in the amount of \$ _____. The

35 penalty provided in this section shall not be construed as restricting any remedy, criminal,
36 provisional, or otherwise, provided by law for the benefit of the agency or any person.
37 (8) The Social Security Administration and the Internal Revenue Service shall adopt any
38 regulations necessary to implement this section.